IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

PATRICK SANTORO, JESSICA LANDIS	:	**CIVIL ACTION**
	:	
	:	
v.	:	**NO. 22-4580**
	:	
TOWER HEALTH	:	

MEMORANDUM

MURPHY, J. **April 24, 2024**

This case invokes fears about the improper sharing of medical information. These days, it is widely understood that when browsing websites, your behavior may be tracked, studied, shared, and monetized. So it may not come as much of a surprise when you see an online advertisement for fertilizer shortly after searching for information about keeping your lawn green. But what about if you visit your hospital's website and browse information about a medical condition that may be of particular concern? This case asks whether a hospital system violates federal privacy and state tort law when it tracks the activity of visitors to its public website. The complaint alleges that a Meta Pixel installed by Tower Health on its own website captured and transmitted HIPAA-protected, individually identifiable health information to Meta without consent.

The plaintiffs' general concern is not frivolous, and cases similar to this one may be found in district courts around the country. But we hold that — in this particular case — plaintiffs' second amended complaint does not explain the nature of the personal information allegedly captured by the Meta Pixel. The specifics are essential to convert a case like this from a law-school hypothetical to an actionable dispute. And because plaintiffs have already had two opportunities to amend their complaint, we will dismiss the action with prejudice.

I. Background[1]

Plaintiffs Patrick Santoro and Jessica Landis are patients of Tower Health and have been Facebook users since before 2018. DI 40 ¶¶ 4, 5.[2] Defendant Tower Health is a regional healthcare provider, with hospitals and urgent care facilities throughout Pennsylvania. *Id*. ¶ 6.

Tower Health maintains a publicly accessible website, towerhealth.org. *Id*. ¶¶ 6, 16, 73. On that website, Tower Health installed software known as Meta Pixel and made by Meta (also known as Facebook).[3] *Id*. ¶ 24. A Meta Pixel is a small piece of code that records information about visitors' activity on a particular webpage. *Id.* ¶¶ 10, 23, 26. The information includes content specific to the user such as IP addresses and Facebook IDs. *Id*. ¶¶ 10, 23, 26. The Meta Pixel also tracks what visitors do on that webpage, including how much time the users spend there or what links they click. *Id*. ¶¶ 10, 23, 26. The Meta Pixel then transmits the recorded information to Meta. *Id*. at 26. Meta in turn analyzes the information for its own commercial purposes, including building a comprehensive profile of the individual user to better target advertisements. *Id*. ¶¶ 11, 12. Meta also releases the data back to the owners of the websites so they can use it for their own commercial purposes. *Id*. ¶ 12.

Because the Meta Pixel captures the "characteristics" and "content" of a visitor's activity on the website, plaintiffs allege this includes a person's individually identifiable health information. *Id.* ¶¶ 26, 27. The second amended complaint illustrates with the following

---

[1] We draw these factual allegations from plaintiffs' second amended complaint. DI 40.

[2] The allegations of Mr. Santoro and Mr. Landis are materially identical for purposes of this motion. We will generally refer to Mr. Santoro for brevity's sake.

[3] Plaintiffs' second amended complaint does not allege that Tower Health embedded the Meta Pixel on its password-protected patient portal, MyTowerHealth. DI 43-2 at 1; DI 40. Hence, there is no allegation that Meta Pixel is accessing those protected medical records.

example. *Id.* ¶ 25. A visitor to Tower Health's website may click on the "Services & Conditions" tab, then click on the "Cancer Care" button, and then select the "Breast Cancer" link. *Id.* This page has buttons that direct users to additional pages providing "information about specific medical conditions, treatment options, services, providers, locations, and clinical trials, many of which have additional links and buttons." *Id.* These pages' URLs[4] convey information about the content of the page. *Id.* For example, the URL of the breast cancer page is https://towerhealth.org/services/breastcancer. *Id.* Because a Meta Pixel captures the URLs visited by a user, the fact that a person has sought information about a specific medical condition is captured and transmitted to Meta. *Id.* ¶ 26.

The plaintiffs "used Tower Health's website to engage in communications that included individually-identifiable health information about [their] past, present, or future health conditions, including requests for information about specific Tower Health providers and locations, and information about specific health conditions, treatments, and medications." *Id.* ¶¶ 43, 49.[5] Tower Health never obtained informed consent or written permission to send supposedly individually identifiable health information to Meta, nor did Tower Health inform the plaintiffs that it would send such information to Meta. *Id.* ¶¶ 45-54.

Tower Health maintains a privacy policy regarding their website which states that Tower Health is "'committed to protecting your online privacy' and that '[i]nformation that Tower

[4] URL means uniform resource locator, better known as a web address, such as https://www.paed.uscourts.gov/.

[5] Regarding the class in general, plaintiffs also allege that Tower "intercepts the characteristics and contents of communications about past, present, and future medical conditions, concerns, symptoms, appointments, providers, treatments, medications, bills, and insurance." *Id.* at ¶ 3.

Health collects on this website will not be sold or given to a third party and will be accessible only by Tower Health.'" *Id.* ¶ 22.

The second amended complaint asserts claims against Tower Health for violation of the Electronic Communications Privacy Act ("Wiretap Act"), negligence, and intrusion upon seclusion. DI 40. It seeks damages, declaratory, and injunctive relief for a class comprising "[a]ll people who used Tower Health's website and had individually identifiable health information . . . shared with Meta without notice or consent." *Id*. ¶ 55.

Tower Health moves to dismiss the second amended complaint in its entirety. DI 43. Among other things,[6] Tower Health argues that the second amended complaint lacks sufficiently specific allegations about what personal health information was transmitted to Meta. DI 43-2; DI 49. This, Tower Health says, undermines all three claims because such "bare, conclusory allegations" do not show it is plausible that, for example, the Meta Pixel actually captured HIPAA protected information as is required for the Wiretap Act claim, that a breach of any duty occurred forming the basis for a negligence claim, or that any intrusion was "highly offensive," constituting intrusion upon seclusion. *Id*.

In response, plaintiffs argue that their complaint contains "detailed, extensive factual allegations" that describe plausible violations of the applicable law. DI 46 at 2. Plaintiffs direct our attention to specific allegations, including a hypothetical example and the fact that the complaint alleges plaintiffs requested information on the website about "Tower Health providers and locations, and information about specific health conditions, treatments, and medications."

[6] Tower Health advances a variety of legal arguments that we needn't address, some of which have spawned differing views among district courts around the country.

Id. at 15, 18. We heard oral argument on March 13, 2024, where, among other things, plaintiffs were given the opportunity to explain what else they might allege if given the opportunity.

II. Analysis

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quotation omitted). A claim has facial plausibility when the facts pleaded permit a court to make the reasonable inference that the defendant is liable for the alleged misconduct. *Id*. The complaint "must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Id*. at 678 (quotation omitted). We take well-pleaded facts to be true, construe those facts in the light most favorable to the plaintiff, and draw reasonable inferences from them. *Connelly v. Lane Constr. Corp*., 809 F.3d 780, 790 (3d Cir. 2016). But "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678.

a. Mr. Santoro's federal Wiretap Act claim fails because he fails to plausibly allege that the Meta Pixel intercepted his individually identifiable health information.

Mr. Santoro alleges that Tower Health violated the Wiretap Act. *See* 18 U.S.C. § 2510. The Wiretap Act forbids any person from "intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept any . . . electronic communication." *Id.* § 2511(1)(a).[7] The Wiretap Act also provides for a private right of action against violators. *Id.* § 2520(a). "[A] plaintiff pleads a prima facie case under the Wiretap Act by showing that the defendant '(1) intentionally (2) intercepted, endeavored to intercept or

[7] The Wiretap Act also forbids "intentionally disclos[ing], or endeavor[ing] to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." *Id.* § 2511(1)(c).

procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device.'" *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 135 (3d Cir. 2015) (quoting *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003)).

Importantly here, the Wiretap Act is a one-party consent statute. It provides that "[i]t shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." § 2511(2)(d). This means that "ordinarily, no cause of action will lie against a private person 'where such person is a party to the communication.'" *Google Inc.*, 806 F.3d at 135.

Mr. Santoro concedes that Tower Health was party to the communications between Mr. Santoro and Towerhealth.org, which means that the one-party consent defense would provisionally apply. DI 43-2 at 7; DI 46 at 8. Thus, the critical question is whether the second amended complaint adequately alleges that Tower Health intercepted the communications "for the purpose of committing any criminal or tortious act." § 2511(2)(d).

To meet the purpose requirement of § 2511(2)(d), Mr. Santoro argues that Tower Health collected data for the purpose of violating the Health Insurance Portability and Accountability Act (HIPAA), which in turn makes it a crime for a person to "knowingly and in violation of this

part . . . disclos[e] individually identifiable health information to another person." 42 U.S.C. § 1320d-6(a)(3); DI 40 ¶¶ 65-69; DI 46 at 8-11.

Mr. Santoro's theory thus requires, among other things, that the information intercepted by Tower Health and transmitted to Meta falls within the scope of HIPAA's definition of "individually identifiable health information." 42 U.S.C. § 1320d-6(a)(3). The HIPAA regulations define individually identifiable health information as "information that is a subset of health information, including demographic information collected from an individual, and: (1) [i] created or received by a health care provider . . . and (2) [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual . . . and (i) [t]hat identifies the individual; or (ii) [w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103; *see Rodriguez v. City of New Brunswick*, 2017 WL 5598217, at *6 (D.N.J. Nov. 21, 2017) (citing to multiple subsections of 45 C.F.R. § 160.103); *Terrell v. Main Line Health, Inc.*, 320 F. Supp. 3d 644, 648 n.2 (E.D. Pa. 2018).

The theory falls short, however, because the second amended complaint lacks specific examples of what HIPAA-protected information from plaintiffs was transferred to Meta. Rather, Mr. Santoro generally avers: "[s]ince 2018, Mr. Santoro has used Tower Health's website to engage in communications that included individually-identifiable health information about his past, present, or future health conditions, including requests for information about specific Tower Health Providers and locations, and information about specific health conditions, treatments, and medications." DI 40 ¶ 43.

For purposes of Mr. Santoro's Wiretap Act theory, these are precisely the kinds of "conclusory or bare-bones allegations" that "will no longer survive a motion to dismiss." *Fowler*

v. UPMC Shadyside, 578 F.3d 203, 210 (3d Cir. 2009). The second amended complaint tells us nothing about the specific pages Mr. Santoro clicked on, his medical condition, or his history of medical care with Tower Health. So, we cannot determine what information Mr. Santoro actually communicated to Tower Health via his web browsing, and thus cannot tell whether that information might be covered by HIPAA. It is interesting to hypothesize about different circumstances that could get the theory into discovery, but the law requires more than hypotheticals at the pleading stage.

Our conclusion is consistent with *Murphy v. Thomas Jefferson University Hospitals, Inc.*, 2023 WL 7017734, at *3 (E.D. Pa. Oct. 10, 2023), which dismissed a similar[8] Wiretap Act claim because the complaint "lack[ed] enough facts to raise a right to relief 'above a speculative level.'" In *Murphy*, the court observed that "plaintiffs do not allege, for example, that any specific test results, diagnoses, or sensitive messages were intercepted or improperly disclosed." *Id.*

Other claims of this sort survived motions to dismiss, but the complaints included more factual details regarding the allegedly intercepted information. For example, in *Cousin v. Sharp Healthcare*, 2023 WL 8007350, at *2-3 (S.D. Cal. Nov. 17, 2023), plaintiffs plausibly alleged that Meta Pixel intercepted HIPAA protected information when they searched for a primary care physician,[9] looked for a doctor who specialized in their particular medical conditions, and booked an appointment to obtain treatment. In another case, the amended complaint alleged that

[8] The allegations in *Murphy* are arguably more specific than those here. In *Murphy*, plaintiffs alleged that their communications were related to their "medical symptoms, conditions, and concerns, medical appointments, medical tests and test results, doctors' visit notes, medications and treatments, and health insurance and medical bills." 2023 WL 7017734, at *3.

[9] Even there, the court noted that this factual allegation "just narrowly survives" dismissal. *Cousin*, 2023 WL 8007350, at *3.

the defendant "transmitted the name and location of her personal physician, as well as her physician's specialty" and included a separate allegation that the information was used by Meta to target her with ads related to her personal health conditions. *Kurowski v. Rush Sys. for Health*, 2023 WL 8544084, at *3 (N.D. Ill. Dec. 11, 2023).

During oral argument, plaintiffs' counsel suggested that the specifics were immaterial because essentially any use of the website necessarily involves the Meta Pixel intercepting and transmitting HIPAA-protected health information. We are unwilling to adopt this conclusion. As best as we can tell from the allegations and undisputed representations, whether individually identifiable health information is intercepted could depend upon how the particular user interacts with the website, including how long they spend on a page, what links are clicked on, and what search terms they input — as well as the nature of the user's health condition and treatment plan. We need not define what constitutes HIPPA-protected information or otherwise flesh out plaintiffs' speculation. It is plaintiffs' responsibility to make factual allegations that plausibly state a claim for relief, and they have not done so here.[10] *See Iqbal*, 556 U.S. at 678. For that reason, we conclude that plaintiffs fail to state a claim for a violation of the Wiretap Act.

b. Mr. Santoro's negligence claim fails because the allegations do not show or infer the existence or breach of a duty of care.

Mr. Santoro's second claim against Tower Health is for negligence. "In Pennsylvania, the elements of negligence are: a duty to conform to a certain standard for the protection of others against unreasonable risks; the defendant's failure to conform to that standard; a causal

[10] Additionally, plaintiffs' privacy-based objections to providing more specificity or context for the bare-bones allegations are not persuasive. There are mechanisms that allow plaintiffs to proceed anonymously or provide sensitive information under seal — some of which have been used in analogous cases. *See Doe v. Regents of Univ. of Cal.*, 672 F. Supp. 3d 813 (N.D. Cal. 2023) (proceeding under a pseudonym); see also *Cousin v. Sharp Healthcare*, 2023 WL 6771573 (S.D. Cal. Oct. 12, 2023) (granting motion by plaintiff to file certain documents under seal).

connection between the conduct and the resulting injury; and actual loss or damage to the plaintiff." *Brewington for Brewington v. City of Philadelphia*, 199 A.3d 348, 356 (Pa. 2018). Mr. Santoro argues that defendant "breached its duty to protect [p]laintiffs' individually-identifiable health information by putting this data to multiple commercial uses without notice and consent." DI 46 at 20. His theory, however, is critically undermined by his failure to adequately plead how Tower Health's public website supposedly collected and transmitted individually identifiable health information.

Certain entities that collect data have a duty to protect that information. *See Dittman v. UPMC*, 196 A.3d 1036, 1047-48 (Pa. 2018) (in a data breach case, imposing a duty on an employer collecting employees' "personal and financial information" to "exercise reasonable care in collecting and storing" the information). But *Dittman*, for example, involved specific sensitive information, including "names, birth dates, social security numbers, addresses, tax forms, and bank account information." *Id.* at 1038. Here, lacking allegations spelling out what information the Meta Pixel collected, we have no basis to conclude that a duty existed to safeguard the information. And if such a duty existed, we cannot assess whether Tower Health breached it by disclosing the information to Meta.[11]

Further, without specific allegations about what information plaintiffs searched on the website (and the consequences of those searches), plaintiffs have not adequately plead causation.

[11] Mr. Santoro also argues that Tower Health's privacy policies and information create a duty not to disclose class members' "individually-identifiable health information" and "medical records." DI 40 ¶¶ 75-82. Like Mr. Santoro's other arguments, this rests on the assumption that Tower Health was collecting such individually identifiable health information and medical records. However, as outlined above, he did not adequately plead this. Although the court in *Murphy* declined to dismiss the negligence claim for failure to allege a duty, citing to plaintiffs' reliance upon the defendant's privacy policies, it did leave open the possibility that it "might resolve the question differently once there is a more fully developed factual record." *Murphy*,

See Murphy, 2023 WL 7017734 at *5 (dismissing a similar negligence claim, in part, because "[p]laintiffs' causation allegations . . . are not sufficiently specific under *Twombly* and *Iqbal*" as they did not describe, in part, the "content, timing, or number of the alleged communications"). Mr. Santoro's second amended complaint similarly rests its causation elements upon broad, conclusory statements. DI 40 ¶ 84. Accordingly, we conclude that the second amended complaint fails to state a negligence claim.

c. Mr. Santoro's intrusion upon seclusion claim fails because the complaint lacks allegations sufficient to find that any intrusion was highly offensive.

Mr. Santoro's final claim is for intrusion upon seclusion, a state law privacy tort that requires him to show "(i) an intentional intrusion (ii) upon the seclusion of another that is (iii) highly offensive to a reasonable person." *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 293 (3d Cir. 2016).[12] To survive dismissal, a plaintiff must "aver sufficient facts to establish that the information disclosed would have caused mental suffering, shame or humiliation to a person of ordinary sensibilities." *Doe v. Hosp. of Univ. of Pa.*, 546 F. Supp. 3d 336, 351 (E.D. Pa. June 29, 2021) (quoting *Pro Golf Mfg., Inc. v. Tribune Rev. Newspaper Co*., 809 A.2d 243, 247 (2002). "[C]ourts may decide the 'highly offensive issue as matter of law at the pleading stage when appropriate.'" *Nickelodeon*, 827 F.3d 262 n.205 (quoting *Boring v. Google, Inc*., 362 F. App'x 273, 279 (3d Cir. 2010)).

2023 WL 7017734, at *4-5. Ultimately, our conclusion is the same regardless of whether Mr. Santoro's reliance upon Tower Health's privacy statements could be enough to establish a duty of care because he has not pleaded causation adequately.

[12] Although *Nickelodeon* was applying New Jersey law, the elements of intrusion upon seclusion are the same in both New Jersey and Pennsylvania; in both states, the tort was derived from the Restatement Second of Torts § 652B. *Hennessey v. Coastal Eagle Point Oil Co.*, 609 A.2d 11, 17 (N.J. 1992); *Taguoma v. Investigative Consultant Servs., Inc.,* 4 A.3d 170, 174 (Pa. Super. Ct. 2010).

The second amended complaint states that Tower Health's intrusion was highly offensive "because it involved intercepting and disclosing the contents of individually-identifiable health information to Meta." DI 40 ¶ 102. However, without any further factual matter describing the information, we hold that the characterization of the alleged intrusion as highly offensive is conclusory and insufficient to state a claim.

Our conclusion mirrors *Murphy*, which dismissed nearly identical allegations because the vague descriptions of health information did not supply "a sufficient factual foundation upon which a reasonable juror could conclude that [the defendant] committed the tort of intrusion upon seclusion." 2023 WL 7017734, at *6. The court held that plaintiffs had "not set forth enough factual matter to cross [the] threshold" to show the conduct was "highly offensive." *Id.* The same is true for Mr. Santoro's claim.

Nickelodeon is also illustrative.[13] In *Nickelodeon*, Plaintiffs were children who alleged that defendants Viacom and Google unlawfully collected their personal information when they visited webpages and watched videos. 827 F.3d at 267. The Third Circuit dismissed an intrusion upon seclusion claim against Google but allowed the claim to proceed against Viacom. It reasoned that simply deploying cookies on a website was not "sufficiently offensive" to survive a motion to dismiss. *Id.* at 294-95. Viacom, however, told parents it was not collecting children's personal information. *Id.* at 295. This, the Third Circuit reasoned, "may have created

[13]Additionally, in *Nickelodeon*, the privacy policy had assured users that it would not track them at all, whereas here, the allegation is that Tower Health's privacy policy assured users only that any information collected by such tracking would not be disclosed to any third parties. 827 F.3d at 269; DI 40 at ¶ 22. Courts in Pennsylvania have held that "liability for intrusion upon seclusion cannot exist where a defendant legitimately obtains information from a plaintiff." *Steinberg v. CVS Caremark Corp.*, 899 F. Supp. 2d 331, 342-43 (E.D. Pa. Feb. 12, 2012). Therefore, this may be another reason plaintiffs cannot sustain a claim for intrusion upon seclusion.

an expectation of privacy" and could constitute the kind of "duplicitous tactics" that made the behavior highly offensive. *Id.*

Lacking allegations about what information Tower Health collected, plaintiffs' situation more closely resembles Google's in *Nickelodeon*. Plaintiffs alleged that their browsing activity was tracked, but there are no factually supported allegations suggesting that this intrusion was "highly offensive" or what information, if any, may have been disclosed in violation of a privacy policy. Our conclusion is also consistent with district court decisions sustaining intrusion upon seclusion claims. A Northern District of California court found that a plaintiff stated a claim with more specific allegations, such as that she had "entered data relating to her heart issues and high blood pressure in MyChart and later received advertisements on Facebook, including at least one advertisement relating to high blood pressure medication." *Doe v. Regents of Univ. of Cal.*, 672 F. Supp. 3d 813, 816, 820 (N.D. Cal. May 8, 2023). Similarly, a Southern District of California court allowed an intrusion upon seclusion claim to proceed where plaintiffs "alleged that their medical conditions and statutes as patients with certain doctors were tracked on [d]efendant's website and transmitted to Meta." *Cousin*, 2023 WL 8007350, at * 3. Mr. Santoro's allegations fall well short of those examples. Thus, we dismiss Mr. Santoro's claim of intrusion upon seclusion.

III. Conclusion

Summing up, we hold that Mr. Santoro's second amended complaint fails to state a claim against Tower Health. And we will dismiss with prejudice. "[T]he grant or denial of an opportunity to amend is within the discretion of the [d]istrict [c]ourt." *Grayson v. Mayview State Hosp.*, 293 F.3d 103, 108 (3d Cir. 2002) (quoting *Foman v. Davis*, 371 U.S. 178, 182 (1962)).

Dismissal with prejudice is appropriate where providing further leave to amend would be futile. See *Lontex Corp., v. Nike, Inc.*, 384 F. Supp. 3d 546, 559 (E.D. Pa. June 10, 2019).

Plaintiffs have had three chances to plead their claims, as well as the opportunity to provide more factual details about the information captured by the Meta Pixel at oral argument. The facts simply aren't there, and therefore, amendment would be futile. We grant Tower Health's motion and dismiss with prejudice.